UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto.gov

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO
90/005,733	05/18/2000	5848259	C72370US	7105

7590 12/01/2003

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
James Seal	
ART UNIT	PAPER NUMBER
2131	31

DATE MAILED: 12/01/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action

Application No. 09/694,416 / 090005733	Applicant(s) Collins et. al.	
Examiner James Seal	Art Unit 2131	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 29 October 2003 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE. Therefore, further action by the applicant is required to avoid abandonment of this application. A proper reply to a final rejection under 37 CFR 1.113 may only be either: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114.

PERIOD FOR REPLY [check either a) or b)]

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) ☐ The period for reply expires on. (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection. ONLY CHECK THIS BOX WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee The appropriate extension fee under 37 CFR 1.17(a) is calculated from. (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b)

1. ☐ A Notice of Appeal was filed on _____. Appellant's Brief must be filed within the period set forth in 37 CFR 1.192(a), or any extension thereof (37 CFR 1.191(d)), to avoid dismissal of the appeal.

2. ☒ The proposed amendment(s) will not be entered because:

   (a) ☒ they raise new issues that would require further consideration and/or search (see NOTE below);

   (b) ☐ they raise the issue of new matter (see Note below);

   (c) ☐ they are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

   (d) ☐ they present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*.

3. ☐ Applicant's reply has overcome the following rejection(s): _____.

4. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

5. ☒ The a)☐ affidavit, b)☐ exhibit, or c)☒ request for reconsideration has been considered but does NOT place the application in condition for allowance because: *See Continuation Sheet*.

6. ☐ The affidavit or exhibit will NOT be considered because it is not directed SOLELY to issues which were newly raised by the Examiner in the final rejection.

7. ☒ For purposes of Appeal, the proposed amendment(s) a)☒ will not be entered or b)☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:

   Claim(s) allowed: _____.

   Claim(s) objected to: *4 and 35*.

   Claim(s) rejected: *1-61*.

   Claim(s) withdrawn from consideration: _____.

8. ☐ The drawing correction filed on _____ is a)☐ approved or b)☐ disapproved by the Examiner.

9. ☐ Note the attached Information Disclosure Statement(s)(PTO-1449) Paper No(s). _____.

10. ☐ Other: _____

Continuation of 2. NOTE: Resubmission does not follow rule that amended portions should be bracketed, e.g. line 16 correction involving lcm not bracketed. .

Continuation of 5. does NOT place the application in condition for allowance because: With regards to new subject matter see Examiner's Action page 7 second paragraph, applicant has not provided support for inclusion of that material (see action for reference to material in question) and the one reference supplied in the original correspondence of applicant supplies one reference in the specification which does not seem to fit any of the matterial which the applicant wishes to add to the specification. With regards to the inclusion of the term digital signature, the examine notes that the private key in a public key system is often used to encrypt with meaning digital signature. Such would be the case of copy protection. The content of the disk is encrypted using the private key while the public key is held by vendors which have signed non-disclosure agreements. The examiner's point is the terms digital signature was not used in the original patent and does not automatically imply digital signature when the private key is used. This also does not cure the problem of the 112 means see page 11 #34. With regards to" extending "versus"using" RSA, the latter being the terminology in the original patent, the examiner notes (see Column 13) that the original RSA patent teaches more than 2 primes and so the applicatant suggesting that his use of more than two is extension of the original RSA does not follow. The original RSA patent teaches both the use of two primes and the use of more than two primes (column 13). With regards to the change of the notation concerning the inequalities, please see Action #15 and note k is the number of primes in n which in applicant specification is Always greater than 2 and yet the proposed change allows the case i = k = 2, which is a contradiction with the first which I do not believe is the intent of the applicant at least from the standpoint of the specification. The examiner thanks the applicant's for suggesting that it is left as in the original. The examier is well aware of the different forms of the CRT and in fact a careful reading of # 16 should reveal this. What the examiner is pointing out in #16 is that the original patent refers to both forms of the CRT, the difficulty is that the part in content seems to follow from the part discussing the use of sumation not iterative or recursive form. With regards to the discussion of randomness page 7 of applicant's correspondence, In re Chu does not apply. We are not talking about selecting three or more random primes as an advantage but as a stated limitation. With regards to RSA/Rivest and Knuth, applicant states that Rivest suggest choosing distinct random primes to protect against sophisticated factoring algorithms. So Rivest clearly teaches random selection of primes is necessary to prevent sophisticated factoring attacks. Selection of random primes would also hold for the same reason in the three or more case even if some of the primes or multiple. With regards to Knuth, Knuth points out that only in the case of distinct primes can the decoding problem be performed using the CRT Alone. In the non-distinct case one must rely on the CRT And the Lemma of Hensel or some equivalent means such as the CRT and p-adics. Clearly, the case that RSA is reciting in Column 13, line 33 RSA refers only to the using Chinese remaindering or its equivalent but does not refer to the added theorems that would be required in the non-distinct prime case. Thus RSA clearly is teaching distinct primes here. The motivation for distinct randomly choosen distinct multiprime comes from the same authors and thus is not pieced together. Knuth is only used to elaborate on the mathematics of the art. With regards to Vanstone and Zuccherator, With regards to Vanstone and Zuccherato, their paper teaches Using four-primes RSA (Column 1, page 2118, pagraphy, note the use of the word "using" RSA as opposed to "extended" RSA) and in particular, the primes (Column 2, page 2118 first complete paragraph teaches that primes of the form p = c + a are selected at random by choosing (selecting Column 2, third paragraph) a random for a given c and then searching for a given prime in the neighborhood. The primes selected in this manner are thus random as there is no determististic distribution of primes known. Again Vanstone et. al. teach the CRT (Column 1, second pargraph page 2118) teaching the use of distinct primes. Hence the four primes of Vanstone et. al. are distinct randomly selected primes. With regards to Nemo, the applicant has alleged that this prior art is sucspect because the original patent listed listed it with no date. The examiner had no difficulty finding a date and reference for this document and does not believe that it should not be considered as art simply because no date was listed in the oin the original patent. As the Applicants claim to have provided this paper, it would help to clear the record if the applicant would provide for the record the origin and probaly date of this article. As the examiner does not see at this time any evidence other than the original patent list it as undated that would disqualify this document the rejection will be maintained pending any information that the applicants might supply on the original and or date of publication. As suggested previously the applicants are encouraged to issue a terminal disclaimer. As far as the journal "Scientific Bulgarian" the examiner will check into this further but the applicant should supply any evidence other than the names that this document should not be taken as face value. With regards to Itakura and Nakamura in view of Rivest, Itukura et. al. is used for the teaching of multiple primes and the teachings of Rivest for random distinct primes as a method to provide a secure public key cryptography.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100